REMARKS

In response to the Office Action mailed on June 23, 2005, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks discussing patentability of rejected and newly added claims. Applicants respectfully request that the application be passed to issue.

Claims 1-43 were previously pending in the subject Application. Claims 44-50 are being added by way of this amendment. Thus, after entry of this Amendment, claims 1-50 will be pending. No new matter was added to the application when amending or adding these claims. Also, the submission of any amendments should not be interpreted as acquiescing to any of the rejections.

The following remarks address the rejections of claims 1-43 as set out in the present Office Action and patentability of newly added claims 44-50. Applicants respectfully request reconsideration.

Summary of an Embodiment of the Invention

Prior to discussion of the pending claims, Applicants would like to briefly discuss an illustrative embodiment of the present invention. One embodiment of the present invention, in contrast to conventional approaches, is directed to techniques for forwarding a request, such as an HTTP request initiated by a client computer, from a network device equipped with the invention, such as a content switch, to a web cache (or other content delivery device such as a web server) that provides a response back to the client without requiring the response to pass through the switch.

As one example approach of the invention, a network device initially receiving the request, such as a content switch or router, can use a special protocol called a "Heads Up Switching Protocol (HUSP)" to forward the request

to the web cache along with additional request information that can include source and destination IP addresses of the request, port information, TCP sequence numbers, client window information (e.g., TCP window information for receiving data), and other related request information, such as HTTP header information all based upon the initial request. The web cache can then use this request information to return content directly back to the client in a HUSP response that is sent to the client without passing through the switch. Thus, the content switch is not burdened with handling all of the responses, and the responses are not delayed due to passing through the content switch. In addition, the HUSP provides a request sequence number that facilitates returning responses from multiple requests by the client in the proper sequence. Thus, the client can provide multiple requests (i.e., pipelined requests) over the same connection to the content switch and can receive responses from the web cache (or other content delivery device) in the same order that the requests were made, without requiring the client to wait until receiving the response to each request before sending another request.

Rejections of Claims 1-36 under 35 U.S.C. § 103(a)

The Examiner has rejected claim 1 under 35 U.S.C. § 103(a) based on the teachings of Brendel et. al, (U.S. Patent 5,774,660) in view of Illnicki, (US. Patent 6,751,677). Applicants are appreciative of the Examiner's review of pending claim 1 and respectfully request further consideration of same in view of the following discussion pointing out why claim 1 is unique and non-obvious over even the combination of cited prior art.

Applicants submit that the current rejection is improper for a number of reasons. First, even the combination of references does not teach or suggest every claim limitation. Second, there is no specific suggestion to combine the techniques in the other reference to render the claim obvious.

1.) Claim 1 includes limitations not found in any of the cited references.

The Examiner notes similarities between the claimed invention and Brendel. Specifically, the Examiner likens the first 3 claim elements (e.g., receiving, providing, and receiving) to the configuration as shown in FIG. 6 of Brendel.

The Examiner admits that Brendel does not expressly teach or suggest the fourth element of "providing a data transfer approval to the data access device in response to receiving the first response, the data transfer approval authorizing the data access device to establish the communication connection to the client based on the connection establishment information and provide a second response to the second request to the client." For this claim limitation, the Examiner cites the title, abstract, FIG. 5, and several passages in Illnicki.

Applicants respectfully submit that the title does not specifically disclose the above technique.

The cited passages include the Abstract in Illnicki, which reads as follows:

> A method of allowing a secure and transparent communication between a user device and servers of a data access network system via a firewall and a gateway is described. The method includes the step of designating a plurality of ports in the firewall for the gateway, each corresponding to one of a number of ports in the gateway. Each of the gateway ports can be dynamically assigned to correspond to the port of one of the servers. The method also includes a step of proxifying an object reference used in a user request for a target server from the user device in order to establish secure connection between the user device and the target server. This step is first performed by replacing the IP address and the port number of the target server of the user request with a dynamically assigned gateway port and the IP address of the gateway. Then the dynamically assigned gateway port and the gateway's IP address are mapped to the port of and IP address of the target server such that the user request is not required to expose the IP address and port number of the target server at the gateway.

This passage does recite a secure connection between a client and a target server through a gateway. However, there is no specific disclosure that that the gateway in Illnicki provides a data transfer approval in response to receiving a communication from the target server. Nor is there a disclosure that the data transfer approval authorizes the data access device to establish the connection with the client.

The Examiner also cites several other passages in Illnicki such as column 3, lines 43-48:

> The method also includes a step of proxifying an object reference that refers to a target server of the servers to be accessed by a user request from the user device in order to allow a single end-to-end secure session between the user device and the target server to be established via the gateway.

column 4, lines 3-7:

> The method also includes a step of proxifying an object reference that refers to the target server to be accessed by a user object invocation request from the user device in order to establish a single end-to-end secure session between the user device and the target server.

column 4, lines 21-30:

> When the user transmits the object invocation request by the client application in the user terminal, a chain of TCP/IP connections (i.e., user terminal-gateway, gateway-gateway, gateway-object) is established from the user terminal. Once such chain of TCP/IP connections is established, the underlying client application in the user terminal establishes over these connections a single SSL session with

the target object server. After the SSL connection is established, the user's object invocation request is sent.

column 5, lines 44-56:

This allows the user object invocation request to be carried over a SSL (Secure Socket Layer) protocol, thus providing end-to-end security (e.g., authentication, confidentiality, and integrity). When the SSL protocol is used, the user terminal 31 and the requested target server are directly mutually authenticated. The confidentiality and integrity is provided from the user terminal 31 to the target server via a single SSL session. This means that the gateway 33 does not need to access the user object invocation request to perform routing as the dynamically assigned port has been mapped to the IP address and port of the target object server. It also means that data can be encrypted end-to-end (i.e., from the user terminal 31 to the target object server).

column 6, lines 25-33:

The firewall 32 is used in the data access network system 30 to control external access (e.g., from the user terminal 31) to the target object servers 34 and/or other data service systems (e.g., e-mail servers) of the data access network system 30. The firewall 32 can be implemented using known firewall technologies. The structure and function of the firewall 32 are well known and thus will not be described in more detail below, except for the portions that relate to the arrangement of the present invention.

Based on contents of these passages, the Examiner argues Illnicki provides "a data transfer approval security feature in order to offer a secure connection through a private networks behind a firewall since security measures are used in data access network system to control external access." In

response to this argument, Applicants point out that these passages in the cited reference merely disclose that it would be useful to provide end-to-end security between a user terminal and a target server through a respective gateway as shown in FIG. 5. Applicants contend that the mere teaching of supporting a secured communication path using a gateway does not teach the unique elements of the claimed invention.

More specifically, Applicants point out that neither Brendel nor Illnicki disclose the specific way of providing the data transfer approval as in the claimed invention. For example, there is no specific disclosure in the passages cited by the Examiner that the gateway in Illnicki receives a response from the target server and, in response to receiving the response from the target server, that the gateway provides the data transfer approval to the target server. Applicants would like to point out that column 8, lines 46-57 (associated with FIG. 5) in Illnicki discloses how the gateway establishes a connection with a target server. However, even this passage does not disclose this element of the claimed invention. The passage at column 8, lines 46-57 reads as follows:

> Because the dynamically assigned gateway port of the gateway 33 and the IP address of the gateway 33 are mapped to the port and IP address of the target server of the servers 34, the gateway 33 then establishes a connection with the target server to authenticate the target server (see FIG. 5). If the target server is not authenticated, the gateway 33 may try to establish a SSL session with the target server using a separate TCP/IP connection. The application layer 62 of the user terminal 31, however, is not aware of how the connection to the target server is established. The SSL "Hello" message is then forwarded to the target server to start a SSL session.

Note that this passage in Illnicki merely indicates that the gateway communicates with the target server to authenticate the target server. Applicants submit that

this teaches away from the claimed invention. For example, the gateway in Illnicki prompts authentication of the target server. As shown in FIG. 5 of Illnicki, the arrow for authentication points from the gateway to the target server, not in the other direction. The claimed invention recites that the data communication device (that the Examiner likens to the gateway in Illnicki) receives a response from the data access device (that the Examiner likens to te target server in Illnicki) and, in response, provides a data transfer approval to the data access device. Thus, mere authentication as discussed in Illnicki is not equivalent to the element in the claimed invention. For example, there is no specific teaching in Illnicki to carry out the claimed technique of providing, from the gateway, a data transfer approval in response to receiving a communication from the target server. In fact, this could not happen because the authentication prompted by the gateway in Illnicki occurs prior to the gateway sending the hello message from the user terminal to the target server. Thus, the target server in Illnicki would not be able to send a communication to the gateway that would prompt the gateway to provide a data transfer approval as a response.

Because the cited reference does not disclose the claim limitation of "providing a data transfer approval to the data access device in response to receiving the first response, the data transfer approval authorizing the data access device to establish the communication connection to the client based on the connection establishment information and provide a second response to the second request to the client," Applicants submit that the Examiner is using the claim language as a blueprint to reject claim 1.

Applicants submit that claim 1 is patentable because it recites a novel and useful technique never used in or even suggested by the prior art. For example, the technique of providing the data transfer approval in response to the communication from the data access device provides a simple "query-response" way of restricting the data access device from servicing a received request (even

though it already has the information to establish a respective connection) until after receiving final approval from the data communication device. Brendel does not recite any way at all to address the issue of final approval at all. Illnicki merely discloses a way of enabling a user terminal to establish a secured connection with a target server through a gateway. Neither reference discloses this simple data transfer approval method.

2.) Illnicki teaches away from the claimed invention.

Applicants would like to further point out, in addition to not reciting every claim limitation as discussed above, that Brendel and Illnicki are not combinable as the Examiner suggests because each reference is directed to solving different problems. For example, Brendel discloses a way for a load balancer to initiate servicing of client requests via communications between a server and a requesting client. Illnicki is directed to setting up a secure connection prior to further communications between the target server.

The Examiner admits that Brendel does not disclose, teach or suggest the claim limitation of: "providing a data transfer approval to the data access device in response to receiving the first response, the data transfer approval authorizing the data access device to establish the communication connection to the client based on the connection establishment information and provide a second response to the second request to the client." The Examiner contends that Illnicki suggests this claim limitation to produce the claimed invention.

Applicants disagree with this contention and respectfully traverse the rejection on the grounds that Illnicki teaches away from such a combination of references to produce the claimed invention. For example, Illnicki does not forward the request (e.g., object invocation) from the gateway to the target server until after the gateway sets up a secure connection between the user terminal and the target server through the gateway. Object invocation is a confidential

communication in Illnicki. As shown in figure 5 of Illnicki, the gateway first authenticates the client. Thereafter, the gateway receives a "Hello" message from the user terminal that has been directed to the target server. The "Hello" message is not a request for data, but is instead an initial communication from the user terminal to invoke a secured connection. As further shown, the gateway then authenticates and thereafter forwards the "Hello" message to the target server. The user terminal and the target server complete a handshake over the secured connection. Finally, the user terminal "invokes the target object" (e.g., sends the request) over the secured connection established by the gateway. See column 8, line 42 to column 9, line 9. At no time during this process does the gateway forward a data request to the target server prior to setting up the secured connection because doing so would put the communication at risk of being discovered. The whole purpose of setting up the secured link between the user terminal and the target server is to prevent non-authorized persons from discovering any data requests and corresponding retrieved data.

Accordingly, Applicants contend that Illnicki can not logically be combined to suggest the claimed invention because Illnicki goes through great lengths to avoid sending a data request to a target server until after establishment of the secured connection. In contradistinction, claim 1 recites that the data communication device forwards the request for data to the data access device before providing the data transfer approval to the data access device. This means that the request for data in the claimed invention is sent to the data access device prior to authorizing the data access device to establish the connection between the data access device and the client. Illnicki therefore teaches away from the claimed invention. That is, there is no indication whatsoever in Illnicki to send an invocation to a target object prior to establishment of a connection between the user terminal and target server. Instead Illnicki teaches that the request is forwarded from the user terminal to the target server after the secured link has been established.

One of ordinary skill in the art may use the technique in Illnicki to set up a secure network connection through a gateway. However, there is no indication in either reference that a data communication device forward "connection establishment information" and thereafter provide a simple "data transfer approval" technique of authorizing a server to service a respective request.

Based on the aforementioned remarks, Applicants respectfully submit that the invention as recited in claim 1 is neither anticipated nor obvious because it includes a unique and useful configuration not taught or suggested by Brenedel, Illnicki or any other reference of record. Thus, in view of the foregoing discussion, Applicants submit that claim 1 in its original form is patentably distinct and advantageous over the cited prior art, and the obviousness rejection should be withdrawn. Accordingly, allowance of claim 1 as well as corresponding dependent claims 2-10 and is respectfully requested.

Claims 11, 21, and 22 include similar limitations as recited in claim 1 above. For applicable reasons as discussed above, claim 10 and corresponding dependent claims 12-20, 37-40, and 45-50 are patentably distinct over the cited prior art.

Claim 3 includes further limitations not disclosed by Cohen. For example, claim 3 recites the steps of "receiving a plurality of first requests to access data from the client;" "providing a plurality of second requests in response to receiving the first requests, each second request including a request sequence number;" and "providing a data transfer approval for each of a plurality of responses to the second requests in a sequence based on the request sequence numbers for the second requests." The Examiner cites additional passages in Brendel and Illnicki to reject this claim. For example, the Examiner contends that Brendel discloses that a sequence number is also included in a TCP/IP header to keep track of

received packets (column 10, lines 31-32). The Examiner cites Brendel at column 12 lines 7-24. Applicants respectfully submit that both of these passages refer to inclusion of sequence numbers associated with multiple packets in one respective communication with the server. That is, Brendel describes how to use sequence numbers to identify portions of communications associated with a same request message. There is no indication whatsoever that that each request includes a request sequence number to distinguish it from the other requests.

In contradistinction, the claimed invention uses sequence numbers to identify that a particular request is one of a sequence of multiple requests received by the data communication device. This enables the data communication device and data access device to more easily keep track of multiple requests and speed up communications. That is, the data communication device and data access device can use the sequence number to identify which request of multiple requests the message pertains. The cited reference provides no indication of this technique because the reference does not address the same communication issue. Illnicki also does not teach use of sequence numbers as in the claimed invention. Applicants therefore respectfully request allowance of dependent claims 3 and 13. Note that newly added claim 45 is allowable for similar reasons.

Regading claim 4, Brendel discloses breaking up a data transmission into multiple packets for a single communication between the load-balancer and one server to which it communicates. In contradistinction, the claimed invention recites that multiple second requests for a single first request are sent to multiple data access devices and thereafter receiving responses from the multiple data access devices. The cited reference only discloses forwarding a request to a single server. Accordingly, Applicants also respectfully request allowance of

claim 4 because it recites limitations not taught or suggested by Brendel or Illnicki.

Claim 6 recites: "wherein the connection establishment information includes a current transmit window for the client that provides a window length for transmitting the second response to the client from the data access device, the window length provided by the client in the first request for use by the data access device when determining a quantity of data to provide in the second response." Applicants have reviewed the cited passage in Brendel at column 10, lines 20-37. This passage merely discloses that a server can break up a file into many data packets when serving a respective client. There is no mention of a current transmit window, a window length, or indication that the client provides an indication of a quantity of data that shall be sent by the data access device to the client in the second response. Applicants therefore respectfully request the allowance of claim 6.

Regarding claim 7, there is no indication in the cited passage that the load balancer notifies a respective server of a client to serve data and a "backup" location identifier of a server that can serve the data if the respective server is unable to service the client. Applicants therefore respectfully request allowance of claim 7 or cite proper language in the prior art teaching such a technique.

Regarding claim 9, the cited passage in Brendel at column 12 lines 7-29 does not disclose the limitations recited in claim 9. For example, the cited passage indicates a standard handshake between the client and the load balancer as indicated at column 12, lines 23-24. Applicants submit that claim 9 recites that the data communication device receives an ACK from the client indicating that the client received a communication from the data access device. Further, claim 9 recites that the data communications device sends an ACK to the data access device so that the data access device receives feedback that the

client received the communication from the data access device. There is no mention in the cited reference that the load balancer sends the server an acknowledgment that the client received a message from the server. Applicants therefore respectfully request the Examiner identify such a specific teaching in the references or allow the claim.

Claims 39 and 43 recite utilization of a sequence number for facilitating servicing of multiple requests from the client to the data communication device. Neither reference discloses this technique of ordering requests. For example, the Examiner cites passages indicating that Brendel uses sequence numbers to label packets for transmission of a file. Applicants request allowance of claim 39 and 43.

Claim 40 recites a specific type of bidding process according to an embodiment of the invention. Neither reference discloses this unique technique of bidding for servicing, especially in the context of servicing the requests other than via communications through the data communication device. For example, Brendel only recites that the load balancer determines which server is best suited to server the request. There is no indication that the load balancer sends performs a bidding process with each server. Thus, Applicants request allowance of claim 40.

Claims 23, 29, 35, and 36 as filed are written from the perspective of a data access device receiving a client request from a data communication device. Claims 23, 29, 35 and 36 include analogous limitations as in claim 1 and are patentably distinct over the cited prior art for similar reasons. Applicants therefore request allowance of claims 23, 29, 35, and 36 as well as respective dependent claims 24-28 and 30-34.

New claim 47

Regarding claims 38 and 42, the Examiner cites Brendel to reject the claimed invention. Applicants submit new claim 47, which indicates that the data communication device forwards the request for data to the data access device prior to establishing a connection between the data access device and the client. For example, as shown in figure 11A, and as discussed in corresponding text, the ordering of forwarding a request and establishing a connection occur in an opposite order as in the claimed invention. That is, Brendel discloses that the load balancer facilitates setting up a connection in step 102 and step 120 and thereafter passes through "a first request" to the server in step 104. The server then responds to the request. Brendel emphasizes that these two processes are not commingled via the dotted line between the two processes. The claimed invention recites an opposite technique. For example, the claimed invention involves forwarding the data request (e.g., indication of the data requested by the client) to the data access device first and thereafter authorizing the data access device to establish a connection with the client. See Brendel column 11, lines 50-63. Brendel therefore teaches away from the claimed invention. Thus, Applicants request allowance of claim 47.

CONCLUSION

In view of the foregoing remarks, Applicants submit that the pending claims as well as newly added claims are in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after reviewing this Response, that the pending claims are not in condition for allowance, the Examiner is respectfully requested to call the Applicant(s) Representative at the number below.

If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-0901.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned Attorney at (508) 366-9600, in Westborough, Massachusetts.

Respectfully submitted,

Paul P. Kriz, Esq.
Attorney for Applicant(s)
Registration No.: 45,752
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 366-9600
Facsimile: (508) 616-9805
Customer No.: 022468

Attorney Docket No.: CIS01-03(3705)

Dated: October 24, 2005